Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

2. Уплотнение информации в аналоговых системах связи [Электронный ресурс]. – 2014. – Режим доступа: http://studopedia.org/2-74270.html – Дата доступа: 11.03.2014.

3. Садомовский, А.С. Приемно-передающие радиоустройства и системы связи / А.С. Садомовский // Ульяновск: УлГТУ, 2007. – 243 с.

4. Тепляков, И.М. Радиолинии космических систем передачи информации / И.М. Тепляков, И.Д. Калашников, Б.В. Рощин // М.: Сов. радио, 1975. – 400 с.

5 Общие положения и классификация методов уплотнения каналов [Электронный ресурс]. – 2011. – Режим доступа: http://www.studfiles.ru/preview/4287735/page:6/ – Дата доступа: 31.05.2015.

О РАЗВИТИИ СРЕДСТВ ДОВЕРЕННОЙ ЗАГРУЗКИ

Д.Ю. СЧАСТНЫЙ

Закрытое акционерное общество «ОКБ САПР»

Средства доверенной загрузки (далее по тексту СДЗ) за последние несколько лет получили существенное развитие. Причин тому видится две: формализация требований к СДЗ со стороны регулятора (ФСТЭК России) и отказ от средств вычислительной техники на базе архитектуры x86 в Государственных Информационных Системах (ГИС) в пользу «альтернативных» архитектур.

Напомню, что с 1 января 2014 года сертификация средств защиты информации, реализующих функции доверенной загрузки, в системе сертификации ФСТЭК России проводится на соответствие Требованиям к средствам доверенной загрузки, утвержденным приказом ФСТЭК России от 27 сентября 2013 г. № 119 [1]. Кроме того, регулятор обязывает применять только сертифицированные средства при построении ГИС и обработке персональных данных [2–3]. Таким образом, разработчики СДЗ получили некоторый формальный набор требований, соответствуя которому, могут называть свой продукт СДЗ. А Заказчики легально применять этот продукт, опираясь на формальное соответствие необходимому классу.

Вторым важным двигателем процесса развития СДЗ видится переход на «альтернативные» архитектуре x86 архитектуры СВТ в ГИС. Такой переход набирает обороты, все чаще в СМИ упоминаются реализованные проекты ГИС, построенные на Эльбрусах, Байкалах или «новой гарвардской архитектуре» [4]. По причине молодости этого рынка СДЗ для них пока очень мало, но создавать их, конечно, необходимо. Причем помимо требований Регулятора, о которых речь шла выше, все-таки основным моментом, мотивирующим Заказчиков ГИС применять СДЗ, должно быть основное предназначение СДЗ – обеспечение доверенной загрузки. При общении с разработчиками и Заказчиками подобных систем можно часто услышать мнение, что применение СДЗ у них необязательно, так как «процессор доверенный, закладок не содержит, враг не пройдет». Но даже самый проверенный процессор с не менее проверенным БИОСом, не содержащим закладок, не выполняет контроль целостности файлов и данных ДО старта операционной системы (ОС). И не производит идентификацию/аутентификацию пользователей ДО старта ОС. И в целом не гарантирует доверенную загрузку ОС. У него другая задача. И именно по этой причине СДЗ нужно применять и на проверенных и доверенных процессорах тоже.

В соответствии в вышеописанными тенденциями можно выделить несколько направлений, по которым идет развитие СДЗ. Во-первых, продолжается развитие традиционных аппаратных СДЗ вслед за развитием средств вычислительной техники

(СВТ). ОКБ САПР традиционно первым выпустил Аккорд-АМДЗ [5] для шины m.2 как ответ на увеличение доли компьютеров с этой новой перспективной шиной. В ближайшие несколько лет, очевидно, все разработчики аппаратных СДЗ будут работать над выпуском своих СДЗ для этой шины.

Третьим потенциальным вектором развития СДЗ может стать СДЗ для шины USB. Несмотря на то, что СДЗ для этой шины разработан уже давно (продукт Инаф ОКБ САПР разработал пять лет назад [6]), в свете требований Регулятора, у него появляется новая ниша. Есть ряд СВТ (например, сервера, терминалы), у которых отсутствуют слоты с шинами расширения типа PCI (USB есть в современных СВТ всегда). Еще одним сценарием применения Инафа может стать встраивание в процесс загрузки «альтернативных» архитектур. Так как процесс загрузки процессоров не x86 достаточно подробно описан и есть возможность легально вносить в него санкционированные изменения, то можно изменить этот процесс таким образом, чтобы загрузка кода СДЗ с USB-устройства производилась в обязательном порядке.

Четвертое направление развития СДЗ связано с программными СДЗ. В приказе №119 выделяются два типа потенциально программных СДЗ: уровня базовой системы ввода-вывода и уровня загрузочной записи. СДЗ уровня загрузочной записи могут быть только низких классов и поэтому вряд ли получат широкое распространение в ближайшее время. А СДЗ уровня базовой системы ввода-вывода потенциально могут использоваться в большинстве ГИС и в системах обработки персональных данных [7]. Внедрение подобных СДЗ в СВТ как архитектуры x86, так и «альтернативных» архитектур достаточно хорошо специфицировано и документировано. В частности, для архитектуры x86 есть стандарт EUFI, который поддерживается большинством современных СВТ этой архитектуры [8]. Способ встраивания в процесс загрузки «альтернативных» архитектур был описан выше и также не представляет особых сложностей. В настоящее время ОКБ САПР начало процесс сертификации СДЗ уровня базовой системы ввода-вывода (под названием Аккорд-МКТ) для процессора Rockchip 3288. Этот СДЗ планируется к использованию на различных устройствах, построенных на «новой гарвардской архитектуре». В первую очередь это будут защищенный терминал «МКТ-card long» и защищенный планшет TrusTPad. Также завершаются работы по разработке аналогичного СДЗ для моноблока «Таволга Терминал» на базе процессора Байкал-Т1. И ведутся работы по встраиванию СДЗ уровня базовой системы ввода-вывода в СВТ на базе процессора Эльбрус. Наряду с этим мы готовим аналогичные СДЗ для EUFI и планируем завершить эту работу к концу лета этого года.

Таким образом можно сказать, что по нашим оценкам СДЗ есть куда развиваться в ближайшее время.

Список литературы

1. Требования к средствам доверенной загрузки, утвержденные приказом ФСТЭК России от 27.09.2013 № 119.

2. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4. Мобильный компьютер с аппаратной защитой доверенной операционной системы. Патент на полезную модель № 138562. 20.03.2014, бюл. № 8.

5. Способ защиты от несанкционированного доступа к информации, хранимой на персональной ЭВМ. Патент на изобретение № 2475823. 20.02.2013, бюл. № 5.

6. Счастный Д. Ю. Привязка облака к земле// Вопросы защиты информации. М., 2015. № 1, с. 45-47.

7. Авезова Я. Э., Фадин А. А. Вопросы обеспечения доверенной загрузки в физических и виртуальных средах// Вопросы кибербезопасности. 2016, № 1(14), с. 24-30.

8. Лыдин С. С. О средствах доверенной загрузки для аппаратных платформ с UEFI BIOS// Вопросы защиты информации: Научно-практический журнал/ФГУП «ВИМИ», М.,2016 г., Вып.3, №114, с. 45-50.

ПРОБЛЕМНЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ ДОВЕРЕННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИНФОРМАЦИОННОМ ВЗАИМОДЕЙСТВИИ СУБЪЕКТОВ РОССИИ И БЕЛАРУСИ

И.М. ТИМЧЕНКО

Оперативно-аналитический центр при Президенте Республики Беларусь

1. Раскрытие отдельных положений межгосударственных соглашений РФ и Беларуси, регулирующих взаимоотношения в сфере защиты информации в части использования средств защиты информации.

2. Описание существующих проблем в области использования средств защиты информации при информационном взаимодействии субъектов РФ и Беларуси.

3. Решение вопросов использовании средств защиты информации и информационных технологий на примерах международного сотрудничества.

4. Возможные направления сотрудничества компетентных органов РФ и Беларуси по оценке средств защиты информации и информационных технологий по требованиям безопасности информации.

Список литературы

1. Соглашение между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области защиты информации (заключено в г. Москве 09.07.1997 г.);

2. Договор о создании Союзного государства (подписан 8 декабря 1999 г. и вступил в силу 26 января 2000 г.).